UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/652,454	08/31/2000	David Cheriton	CISCP537	3379

26541 7590 03/01/2006

Cindy S. Kaplan
P.O. BOX 2448
SARATOGA, CA 95070

EXAMINER	
SIMITOSKI, MICHAEL J	
ART UNIT	**PAPER NUMBER**
2134	

DATE MAILED: 03/01/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/652,454	CHERITON, DAVID	
	Examiner	Art Unit	
	Michael J. Simitoski	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 December 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3,4,6-8,10,11,14,15,17-21,23-30 and 32-41* is/are pending in the application.

4a) Of the above claim(s) *39-41* is/are withdrawn from consideration.

5)☒ Claim(s) *1,3,4,6-8,10,11,14,18-21,23-27,35,37 and 38* is/are allowed.

6)☒ Claim(s) *15,17,28,29,32-34 and 36* is/are rejected.

7)☒ Claim(s) *30* is/are objected to.

8)☒ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. The response of 12/21/2005 was received and considered.

2. Claims 1, 3-4, 6-8, 10-11, 14-15, 17-21, 23-30 & 32-41 are pending.

3. Claims 1, 3-4, 6-8, 10-11, 14, 18-21, 23-27, 35 & 37-38 are allowed, claims 1 & 30 are objected to, claims 15, 17, 28-29, 32-34 & 36 are rejected and claims 39-41 are constructively elected by original presentation for prosecution.

Response to Arguments

4. Applicant's arguments filed 10/27/2005 have been fully considered but they are not fully persuasive.

Applicant's response (p. 9) argue that support for identifying if a rate of traffic exceeds a sampling capability of the aggregate filter exists in the specification. However, it is maintained that the specification does not enable one of ordinary skill to determine the sampling capability of an aggregate filter.

Applicant's response (p. 10) argues that the 101 rejections are overcome. However, the claimed recording medium is still non-functional, not requiring an interrelationship between the medium and the data.

Regarding claims 28-29, Cheriton discloses receiving data at a network device (p. 8, ¶2), classifying network flows based on one or more packets received at the network device (p. 8, ¶2), analyzing one or more of said network flows (p. 8, ¶3) and processing each of said network flows according to a corresponding policy (p. 8, ¶2). Cheriton lacks selecting a class of network flows to analyze. However, Romig teaches that aggregating subsequent traffic in flow logs (p. 3,

¶2) is beneficial because they can be used for intrusion detection (analyze for potentially harmful flows) (p. 5, ¶1). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Cheriton to select and analyze a class of network flows. One of ordinary skill in the art would have been motivated to perform such a modification to allow for intrusion detection by examining the flow summaries, as taught by Romig (p. 3, ¶2 & p. 5, ¶1). Cheriton lacks generating a filter for said one or more network flows and refining said filter for said selected class of network flows. However, Smith teaches a firewall that works with intrusion detection software to automatically cause a set of firewalls to dynamically change their security policy (generate or refine a filter) for individual attack activity (p. 494, col. 1, ¶3) and add additional rules (§3.3 #3 & p. 498 ¶2) to push the protection to a point nearer to the hacker (p. 496, col. 2, last ¶ & p. 498, ¶2). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Cheriton to generate a filter corresponding to detected potentially harmful network flows to prevent packets from passing through the network device. One of ordinary skill in the art would have been motivated to perform such a modification to push the protection to a point nearer to the hacker, as taught by Smith (p. 494 col. 1 ¶3, p. 496 col. 2 last ¶ & p. 498 ¶2).

Election/Restrictions

5. Newly submitted claims 39-41 directed to an invention that is independent or distinct from the invention originally claimed for the following reasons: The newly submitted claims recite refining a plurality of aggregate filters and monitoring statistics associated with said plurality of aggregate filters and creating a network flow for packets passing through a first

aggregate filter (classified in 370/230.1) and are related to the original claims as subcombinations usable together and have separate utility such as vulnerability assessment. The newly submitted claims do not require generating filters by analyzing traffic for potentially harmful packets (classified in 726/23) and do not require classifying network flows based on one or more packets received at a device (classified 713/154).

Since applicant has received an action on the merits for the originally presented invention, this invention has been constructively elected by original presentation for prosecution on the merits. Accordingly, claims 39-41 are withdrawn from consideration as being directed to a non-elected invention. See 37 CFR 1.142(b) and MPEP § 821.03.

Claim Objections

6. Claim 1 is objected to because of the following informalities:

Regarding claim 1, "aggregate network flow summaries" (line 7) should be replaced with "aggregate network flow summary".

Regarding claim 1, "to network flow" (line 14) should be replaced with "to a network flow".

Appropriate correction is required.

Claim Rejections - 35 USC § 101

7. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

8. Claims 15, 17 & 36 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claim 15 is a computer product on a computer-readable storage medium, including a data signal embodied on a carrier wave, not having a functional interrelationship with a computer or the medium.

Specification

9. The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required: The specification does not explicitly disclose the limitation "wherein the computer-readable storage medium is not a data signal".

Claim Rejections - 35 USC § 112

10. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

11. Claims 15, 17 & 36 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. The specification does not explicitly disclose the limitation "wherein the computer-readable storage medium is not a data signal".

12. Claims 32-34 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. The specification does not enable one of ordinary skill in the art to identify if a rate of traffic exceeds a sampling capability of the aggregate filter.

13. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

14. Claims 3-4, 6 & 8 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Regarding claim 3, the limitation "is classified based on" lacks proper antecedent basis.

Regarding claim 4, the limitation "is classified based on" lacks proper antecedent basis.

Regarding claim 6, the limitation "wherein analyzing at least one of said network flows" lacks proper antecedent basis.

Regarding claim 8, the limitation "wherein sending each ..." lacks proper antecedent basis.

Regarding claim 8, the limitation "analyzing said network flow" lacks proper antecedent basis.

Claim Rejections - 35 USC § 103

15. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

16. Claims 28 & 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over WO 97/24841 to Cheriton et al. (**Cheriton**) in view of "Cisco Flow Logs and Intrusion Detection at the Ohio State University" by Romig et al. (**Romig**) in view of "Operating Firewalls Outside the LAN Perimeter" by Smith et al. (**Smith**).

Regarding claims 28 & 29, Cheriton discloses receiving data at a network device (p. 8, ¶2), classifying network flows based on one or more packets received at the network device (p. 8, ¶2), analyzing one or more of said network flows (p. 8, ¶3) and processing each of said network flows according to a corresponding policy (p. 8, ¶2). Cheriton lacks selecting a class of network flows to analyze. However, Romig teaches that aggregating subsequent traffic in flow logs (p. 3, ¶2) is beneficial because they can be used for intrusion detection (analyze for potentially harmful flows) (p. 5, ¶1). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Cheriton to select and analyze a class of network flows. One of ordinary skill in the art would have been motivated to perform such a modification to allow for intrusion detection by examining the flow summaries, as taught by Romig (p. 3, ¶2 & p. 5, ¶1). Cheriton lacks generating a filter for said one or more network flows and refining said filter for said selected class of network flows. However, Smith

teaches a firewall that works with intrusion detection software to automatically cause a set of firewalls to dynamically change their security policy (generate or refine a filter) for individual attack activity (p. 494, col. 1, ¶3) and add additional rules (§3.3 #3 & p. 498 ¶2) to push the protection to a point nearer to the hacker (p. 496, col. 2, last ¶ & p. 498, ¶2). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Cheriton to generate a filter corresponding to detected potentially harmful network flows to prevent packets from passing through the network device. One of ordinary skill in the art would have been motivated to perform such a modification to push the protection to a point nearer to the hacker, as taught by Smith (p. 494 col. 1 ¶3, p. 496 col. 2 last ¶ & p. 498 ¶2).

Allowable Subject Matter

17. Claims 1, 3-4, 6-8, 10-11, 14, 18-21, 23-27, 35 & 37-38 are allowed.

18. Claims 15, 17 & 36 would be allowable if rewritten or amended to overcome the rejection(s) under 35 U.S.C. 112, 2nd paragraph, set forth in this Office action.

19. Claim 30 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

20. The following is a statement of reasons for the indication of allowable subject matter:

a. Regarding claims 1 & 15, Romig discloses separating data into a plurality of network flows (p. 2, ¶4-6), creating separate aggregate network flow summaries/flow logs for each of said network flows (p. 3, ¶1), sending at least one of said aggregate network flow summaries to a flow analyzer/Flow-dscan (p. 5, ¶1), analyzing said at least

one aggregate network flow summary (p. 5, ¶1) to detect characteristics of potentially harmful network flows (p. 5, ¶1) and selecting a new aggregate network flow summary to analyze (p. 5, ¶2). Smith discloses generating a filter (a processing rule) and refining the filter (adding additional rules) (pp. 494, 496 & 498). However, Romig, as modified above, discloses performing the analysis at more powerful system, rather than at the network device and discloses sending additional flow summaries to an analyzer, hence lacking sending the selected aggregate network flow summary to the flow analyzer for analysis, wherein the new aggregate flow summary explicitly corresponds to network flow associated with the generated or refined filter.

b. Regarding claim 18, Romig discloses a netflow device operable to receive streams of packets, separate said streams (p. 2, ¶4-6), and create a summary record/flow logs containing information on each of said streams (p. 3, ¶1), a flow analyzer/Flow-dscan (p. 5, ¶1) operable to receive said summary records/Flow logs from said netflow device and analyze said summary records and identify potentially harmful network flows (p. 5, ¶1). Smith discloses generating a filter (a processing rule) (pp. 494, 496 & 498). However, Romig, as modified above, discloses performing the analysis at more powerful system, rather than at the network device and discloses creating new summary records of flows removed from the cache, hence lacking the netflow device being operable to create a new summary record explicitly containing information on a stream of data associated with said generated or refined filter.

c. Regarding claim 30, the prior art relied upon fails to teach or suggest generating filters specifically for a corresponding network flow, refining the filter and modifying the classification of flows, in combination with the other elements of the claims.

Conclusion

21. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

22. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (571) 272-3841. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m.. The examiner can also be reached on alternate Fridays from 6:45 a.m. – 3:15 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached at (571) 272-3838.

Any response to this action should be mailed to:
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450
Or faxed to:
(571) 273-8300
(for formal communications intended for entry)
Or:
(571) 273-3841 (Examiner's fax, for informal or draft communications, please label "PROPOSED" or "DRAFT")

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2100.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MJS
February 22, 2006

GILBERTO BARRÓN JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100